CLAIMS

What is claimed is:

1. A method for providing path-level access control to a structured document in a collection stored in a database, wherein the structured document comprises a plurality of nodes, comprising the steps of:

a) providing an access control policy for the collection, wherein the access control policy comprises a plurality of access control rules;

b) generating a path for each node of the plurality of nodes in the document; and

c) generating for each path associated with a node a corresponding value expression based on at least one access control rule of the plurality of access control rules,

wherein the corresponding value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

2. The method of claim 1, wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node.

3. The method of claim 1 further comprising:

(d) storing each path and the corresponding value expression in a table.

4. The method of claim 3 further comprising:

(e) compiling each value expression prior to storing step (d).

5. The method of claim 4 further comprising:

(f) receiving a query from a user, wherein the query requests access to a node in the document;

(g) executing the query;

(h) evaluating the value expression corresponding to the path associated with the requested node;

(i) displaying data associated with the requested node if the value expression grants access to the user; and

(j) hiding data associated with the requested node if the value expression denies access to the user.

6. The method of claim 5, wherein the evaluating step (h) is performed during a run time.

7. The method of claim 1, wherein generating step (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path.

8. The method of claim 3, further comprising:

(e) replacing the value expression for a path associated with a node with a reference notation if the value expression is identical to that for a path associated with the node's parent, thereby eliminating repeated value expressions in the table.

9. The method of claim 1, wherein the providing step (a) comprises:

(a1) writing the plurality of access control rules; and

(a2) validating the plurality of access control rules such that the resulting rules are syntactically and logically valid.

10. The method of claim 1, wherein the structured document is written in Extensible Markup Language.

11. A computer readable medium containing programming instructions for providing path-level access control to a structured document in a collection stored in a database, wherein the structured document comprises a plurality of nodes, instructions for:

a) providing an access control policy for the collection, wherein the access control policy comprises a plurality of access control rules;

b) generating a path for each node of the plurality of nodes in the document; and

c) generating for each path associated with a node a corresponding value expression based on at least one access control rule of the plurality of access control rules,

wherein the corresponding value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

12. The computer readable medium of claim 11, wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node.

13. The computer readable medium of claim 11 further comprising:

(d) storing each path and the corresponding value expression in a table.

14. The computer readable medium of claim 13 further comprising:

(e) compiling each value expression prior to storing instruction (d).

15. The computer readable medium of claim 14 further comprising:

(f) receiving a query from a user, wherein the query requests access to a node in the document;

(g) executing the query;

(h) evaluating the value expression corresponding to the path associated with the requested node;

(i) displaying data associated with the requested node if the value expression grants access to the user; and

(j) hiding data associated with the requested node if the value expression denies access to the user.

16. The computer readable medium of claim 15, wherein the evaluating instruction (h) is performed during a run time.

17. The computer readable medium of claim 11, wherein generating instruction (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules associated with each path into a statement indicating who is granted and denied access to the path.

18. The computer readable medium of claim 13, further comprising:

(e) replacing the value expression for a path associated with a node with a reference notation if the value expression is identical to that for a path associated with the node's parent, thereby eliminating repeated value expressions in the table.

19. The computer readable medium of claim 11, wherein the providing instruction (a) comprises:

(a1) writing the plurality of access control rules; and

(a2) validating the plurality of access control rules such that the resulting rules are syntactically and logically valid.

20. The computer readable medium of claim 11, wherein the structured document is written in Extensible Markup Language.

21. A system for providing path-level access control to a structured document in a collection stored in a database, wherein the structured document comprises a plurality of nodes, comprising:

a database management system in a computer system;

an access control policy for the collection, wherein the access control policy comprises a plurality of access control rules; and

an Access Control mechanism in the database management system for generating a path for each node of the plurality of nodes in the document, and for generating for each path associated with a node a corresponding value expression based on at least one access control rule of the plurality of access control rules,

wherein the database management system utilizes the corresponding value expression during access control evaluation to determine whether a user is allowed to access a node in the structured document..

22. The system of claim 21, wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node.

23. The system of claim 21 wherein the Access Control mechanism is configured to store each path and the corresponding value expression in a table.

24. The system of claim 23 further comprising a compiler for compiling each value expression prior to storing in the table.

25. The system of claim 24 wherein the database management system is configured to receive a query from a user, wherein the query requests access to a node in the document, to execute the query, to evaluate the value expression corresponding to the path associated with the requested node, to display data associated with the requested node if the value expression grants access to the user, and to hide data associated with the requested node if the value expression denies access to the user.

26. The system of claim 25, wherein access control evaluation is performed during a run time.

27. The system of claim 21, wherein the access control mechanism comprises:

a translator for normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path, and for propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

a value expression generator for transforming each of the at least one access control rules associated with each path into a statement indicating who is granted and denied access to the path.

28. The system of claim 21, wherein the access control rules are syntactically and logically valid.

29. The system of claim 21, wherein the structured document is written in Extensible

Markup Language.

30. A method for providing path-level access control to a structured document in a collection stored in a database, wherein the structured document comprises a plurality of nodes, comprising the steps of:

a) providing an access control policy for the collection, wherein the access control policy comprises a plurality of access control rules;

b) generating a path for each node of the plurality of nodes in the document;

c) generating for each path associated with a node a corresponding value expression based on at least one access control rule of the plurality of access control rules, wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node; and

(d) storing each path and the corresponding value expression in a table;

wherein the corresponding value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

31. The method of claim 30 further comprising:

(e) receiving a query from a user, wherein the query requests access to a node in the document;

(f) executing the query;

(g) evaluating the value expression corresponding to the path associated with the requested node during a run time;

(h) displaying data associated with the requested node if the value expression grants

access to the user; and

(i) hiding data associated with the requested node if the value expression denies access to the user.

32. The method of claim 30, wherein generating step (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path.

33. A computer readable medium containing programming instructions for providing path-level access control to a structured document in a collection stored in a database, wherein the structured document comprises a plurality of nodes, the programming instructions for:

a) providing an access control policy for the collection, wherein the access control policy comprises a plurality of access control rules;

b) generating a path for each node of the plurality of nodes in the document;

c) generating for each path associated with a node a corresponding value expression based on at least one access control rule of the plurality of access control rules, wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node; and

(d) storing each path and the corresponding value expression in a table;

wherein the corresponding value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

34. The computer readable medium of claim 33 further comprising:

(e) receiving a query from a user, wherein the query requests access to a node in the document;

(f) executing the query;

(g) evaluating the value expression corresponding to the path associated with the requested node during a run time;

(h) displaying data associated with the requested node if the value expression grants access to the user; and

(i) hiding data associated with the requested node if the value expression denies access to the user.

35. The computer readable medium of claim 33, wherein generating instruction (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each

path into a statement indicating who is granted and denied access to the path.

36. A method for providing path-level access control to a structured document in a collection stored in a database, wherein the structured document comprises a plurality of nodes, comprising the steps of:

a) providing an access control policy for the collection, wherein the access control policy comprises a plurality of access control rules;

b) generating a path for each node of the plurality of nodes in the document;

c) generating for each path associated with a node a corresponding value expression based on at least one access control rule of the plurality of access control rules, wherein the generating step comprising:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path; and

(d) storing each path and the corresponding value expression in a table;

wherein the corresponding value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

37. A computer readable medium containing programming instructions for providing

path-level access control to a structured document in a collection stored in a database, wherein the structured document comprises a plurality of nodes, the programming instructions for:

a) providing an access control policy for the collection, wherein the access control policy comprises a plurality of access control rules;

b) generating a path for each node of the plurality of nodes in the document;

c) generating for each path associated with a node a corresponding value expression based on at least one access control rule of the plurality of access control rules, wherein the generating step comprising:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path; and

(d) storing each path and the corresponding value expression in a table;

wherein the corresponding value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.